OIPE JC160
MAR 2 4 2004
PATENT & TRADEMARK OFFICE

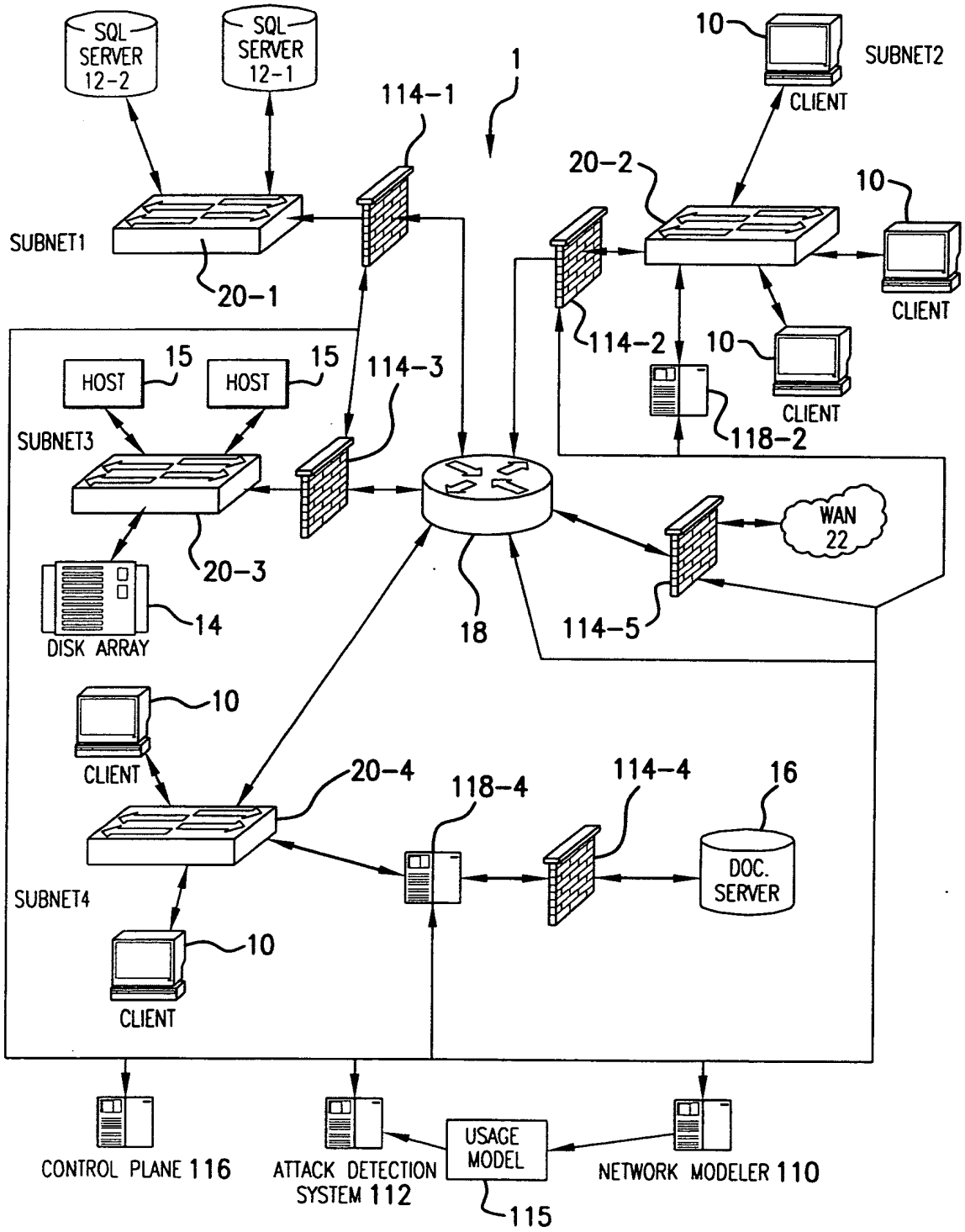

FIG. 1

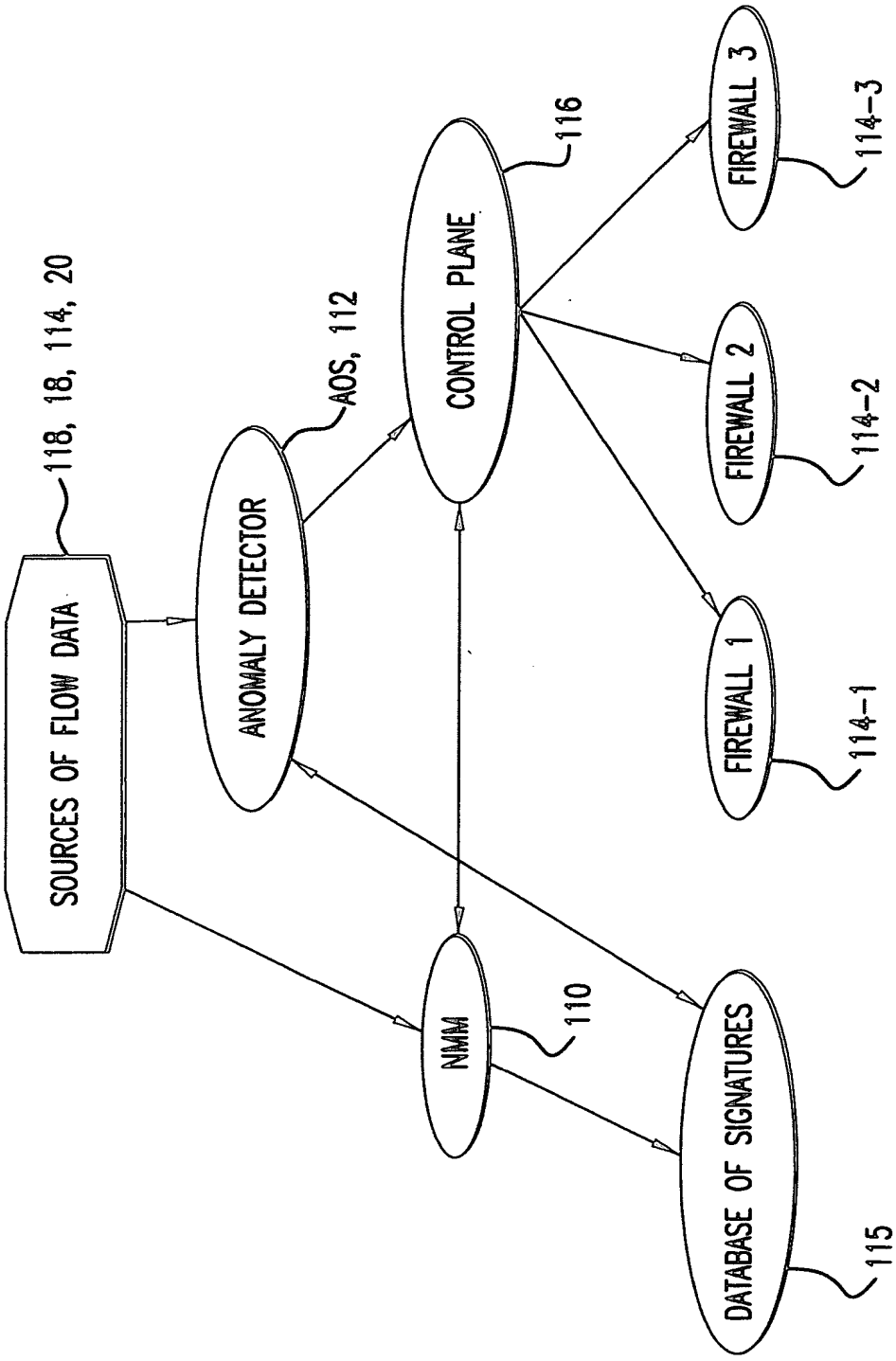
SOURCES OF FLOW DATA
118, 18, 114, 20
ANOMALY DETECTOR
AOS, 112
CONTROL PLANE
116
FIREWALL 1
114-1
FIREWALL 2
114-2
FIREWALL 3
114-3
NMM
110
DATABASE OF SIGNATURES
115

FIG. 2

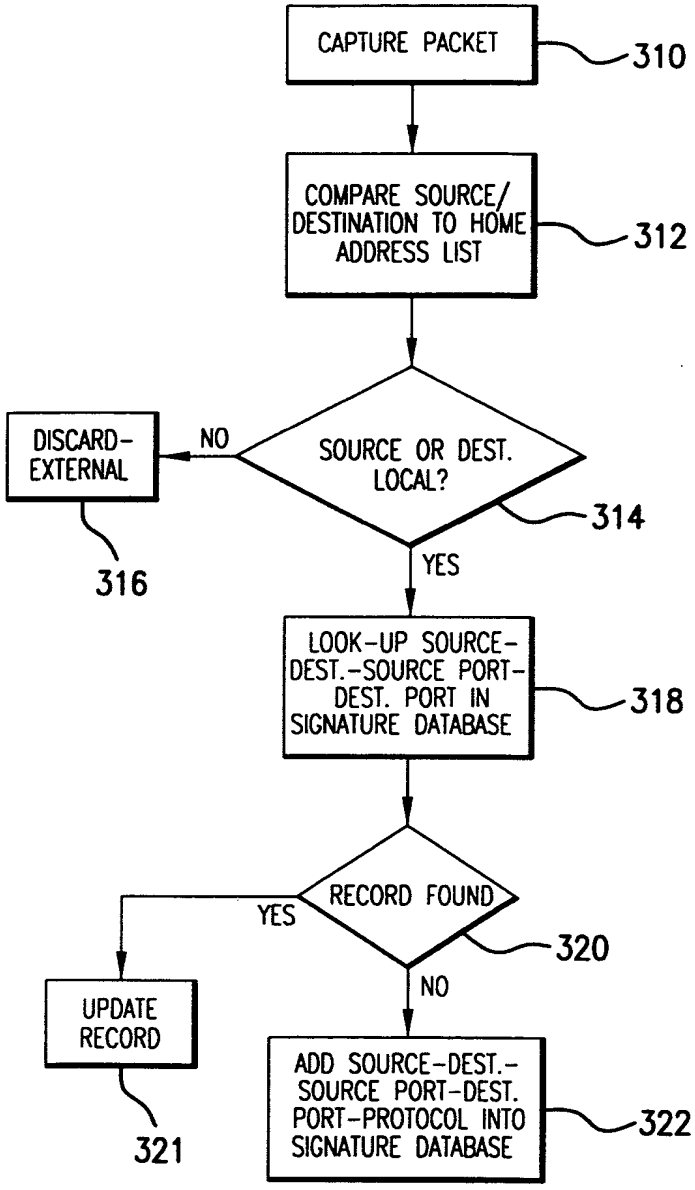
CAPTURE PACKET
310
COMPARE SOURCE/ DESTINATION TO HOME ADDRESS LIST
312
SOURCE OR DEST. LOCAL?
314
NO
DISCARD-EXTERNAL
316
YES
LOOK-UP SOURCE-DEST.-SOURCE PORT-DEST. PORT IN SIGNATURE DATABASE
318
RECORD FOUND
320
YES
NO
UPDATE RECORD
321
ADD SOURCE-DEST.-SOURCE PORT-DEST. PORT-PROTOCOL INTO SIGNATURE DATABASE
322

FIG.3

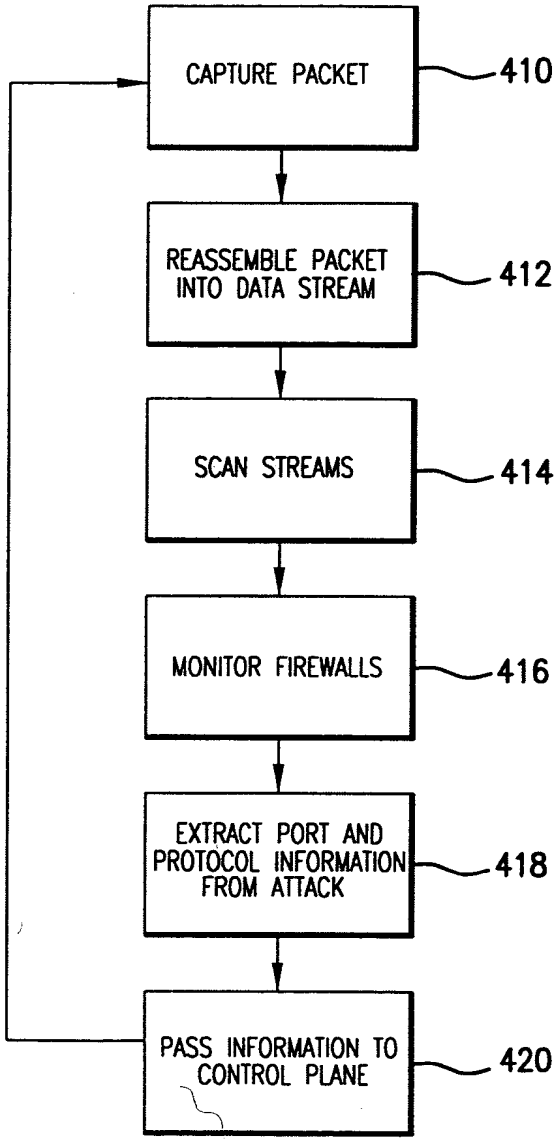
CAPTURE PACKET
410
REASSEMBLE PACKET INTO DATA STREAM
412
SCAN STREAMS
414
MONITOR FIREWALLS
416
EXTRACT PORT AND PROTOCOL INFORMATION FROM ATTACK
418
PASS INFORMATION TO CONTROL PLANE
420

FIG.4A

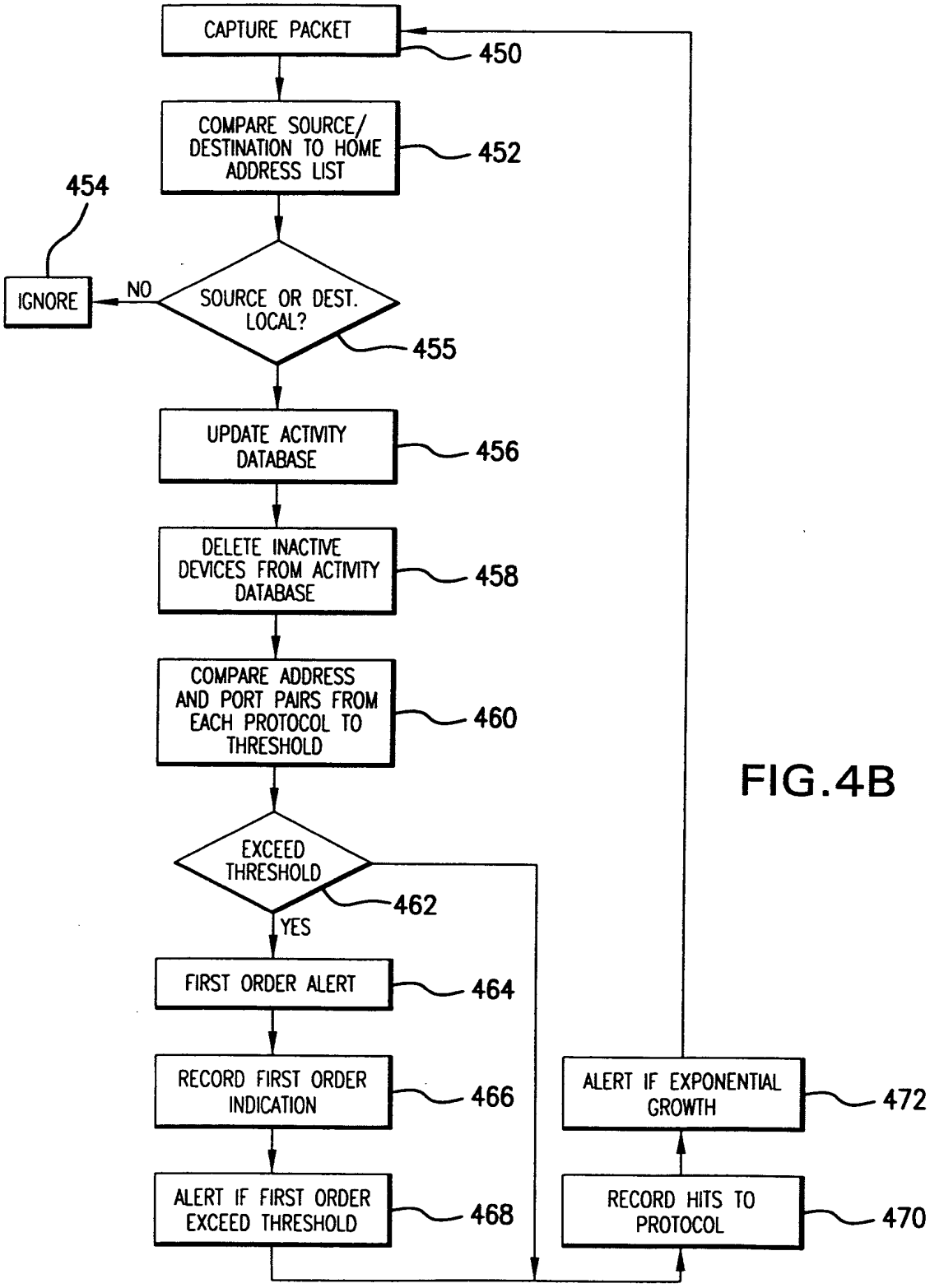
CAPTURE PACKET
450
COMPARE SOURCE/ DESTINATION TO HOME ADDRESS LIST
452
454
IGNORE
NO
SOURCE OR DEST. LOCAL?
455
UPDATE ACTIVITY DATABASE
456
DELETE INACTIVE DEVICES FROM ACTIVITY DATABASE
458
COMPARE ADDRESS AND PORT PAIRS FROM EACH PROTOCOL TO THRESHOLD
460
EXCEED THRESHOLD
462
YES
FIRST ORDER ALERT
464
RECORD FIRST ORDER INDICATION
466
ALERT IF FIRST ORDER EXCEED THRESHOLD
468
ALERT IF EXPONENTIAL GROWTH
472
RECORD HITS TO PROTOCOL
470

FIG.4B

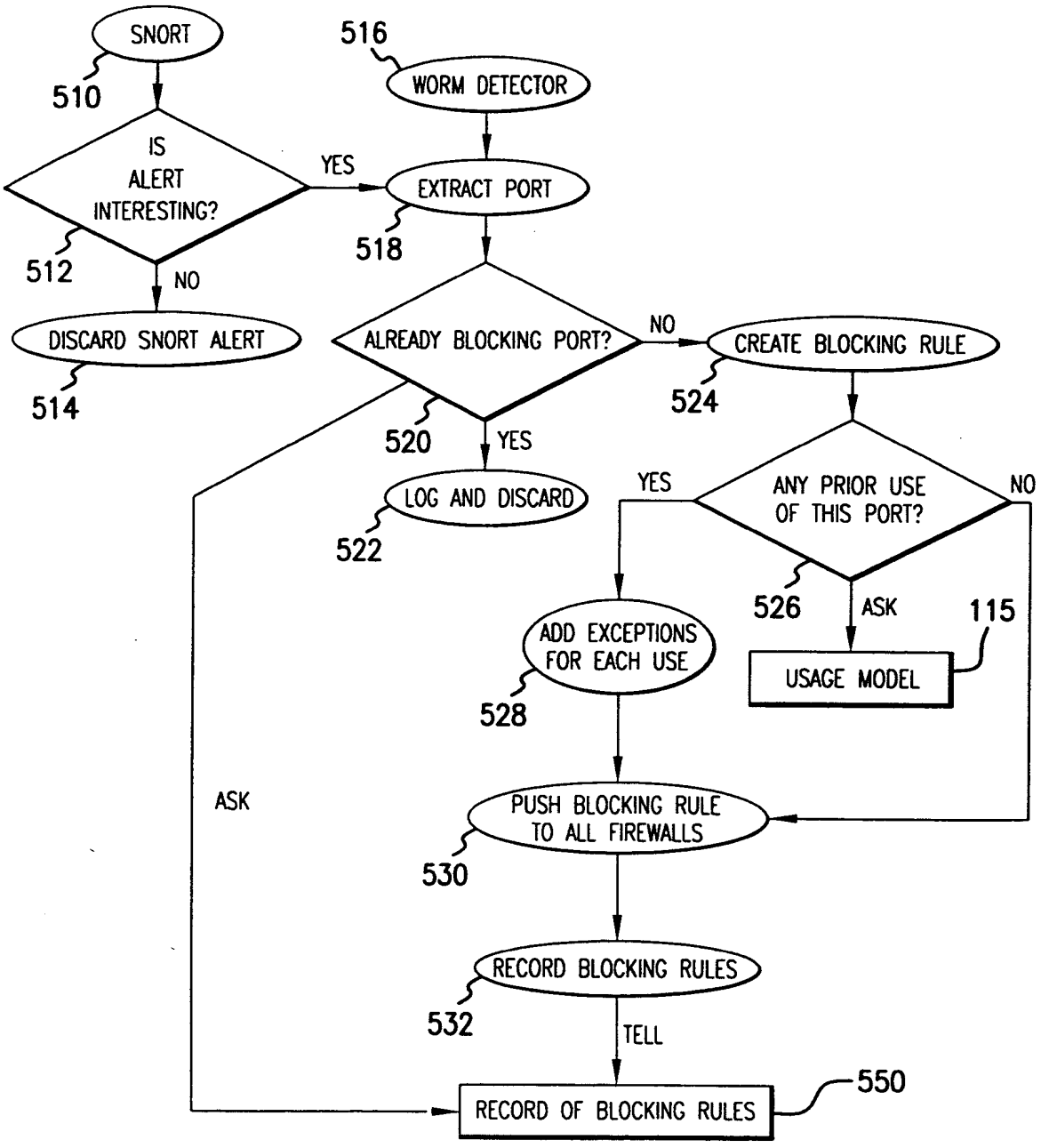
SNORT
510
516
WORM DETECTOR
IS ALERT INTERESTING?
YES
EXTRACT PORT
512
518
NO
DISCARD SNORT ALERT
514
ALREADY BLOCKING PORT?
NO
CREATE BLOCKING RULE
524
520
YES
LOG AND DISCARD
522
YES
ANY PRIOR USE OF THIS PORT?
NO
526
ASK
115
USAGE MODEL
ADD EXCEPTIONS FOR EACH USE
528
ASK
PUSH BLOCKING RULE TO ALL FIREWALLS
530
RECORD BLOCKING RULES
532
TELL
RECORD OF BLOCKING RULES
550

FIG.5